Inj. one way, surj. other way

$$\begin{gathered} A, B \text{ sets}, A \neq \emptyset \\ \exists \text{ inj } A \hookrightarrow B \iff \exists \text{ surj } B \twoheadrightarrow A \end{gathered} \tag{1}$$

Proof: ($\Longrightarrow$) Suppose we have inj $i : A \hookrightarrow B$. We can restrict the cod(i) to get a bij.

$$i' : A \hookrightarrow \text{range}(i) \tag{2}$$

i' has an inverse $i'^{-1} : \text{range}(i) \to A$.

$$\begin{gathered} f : B \to A \\ f(b) = \begin{cases} i'^{-1} & \text{if } b \in \text{range}(i) \\ a & \text{otherwise} \end{cases} \end{gathered} \tag{3}$$

($\Longleftarrow$) Suppose we have surj $s : B \twoheadrightarrow A$.

For each $a \in A$, pick $f(a) \in s^{-1}(a)$. This defines $f : A \hookrightarrow B$. □

Cantor-Schröder-Bernstein

$$\begin{gathered} \text{If } \exists \text{ inj } A \hookrightarrow B \\ \text{and } \exists \text{ inj } B \hookrightarrow A \\ \text{then } \exists \text{ bij } A \to B \end{gathered} \tag{4}$$

Finiteness

A is finite when $|A| = |\underline{n}|, n \in \mathbb{N}$. $\underline{0} = \emptyset$.

Infiniteness

1. A is infinite if A is not finite.

$$|A| \neq |\underline{n}| \ \forall n \in \mathbb{N} \cup \{0\} \tag{5}$$

2. A is *Dedekind infinite* if there exists a proper subset $A_1 \subsetneq A$ such that $|A| = |A_1|$.
3. A is infinite if $|\mathbb{N}| \leq |A|$. In other words, if it is at least as big as the natural numbers, which is the smallest infinite set.

Shifting Formula

$$\begin{gathered} \text{bij } f : (a, b) \to (c, d) \\ f(x) = \frac{x - a}{b - a}(d - c) + c \end{gathered} \tag{6}$$

Induction

If $A \subseteq \mathbb{N}$ is inductive and $1 \in A$, then $A = \mathbb{N}$.

Contrapositive

$$P \Longrightarrow Q \iff \neg Q \Longrightarrow P \tag{7}$$

Contradiction

To prove P, assume $\neg P \Longrightarrow$ something impossible.

Example with primes

There are ∞ many primes.

Proof: Suppose there are finite primes. Then, we can list them $p_1, p_2, ..., p_n$.

Consider $a = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$. Then (with assumptions of finite primes) a is not prime because a is larger than any of the finite number of primes we have. In other words, $\frac{a}{p_k} \in \mathbb{Z}$ for some k.

$$\begin{aligned} \frac{a}{p_k} &= \underbrace{p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_{k-1} \cdot p_{k+1} \cdot ...}_{\text{integers}} + \underbrace{\frac{1}{p_k}}_{\text{not int}} \\ &= \frac{a}{p_k} : \text{must not be an int} \end{aligned} \tag{8}$$

But we said that $\frac{a}{p_k}$ must be an integer, which leads to a contradiction ↯. □

Countable Sets

A is countable if $|A| = |\underline{n}|$ or $|A| = |\mathbb{N}|$. Same as $|A| \leq |\mathbb{N}|$.

A, B countable $\Longrightarrow A \cup B$ countable.

$$|\underline{n}| \leq |\underline{m}| \iff n \leq m \tag{9}$$

$$\forall n \in \mathbb{N} \cup \{0\}, |\underline{n}| < |\mathbb{N}| \tag{10}$$

Bigger Sets

$A \neq \emptyset, |\mathscr{P}(A)| > |A|$.

Proof: $|A| \leq |\mathscr{P}(A)|$ means we have an injection $A \hookrightarrow \mathscr{P}(A)$, where $a \mapsto \{a\}$.

WTS that $\nexists$ surj. $A \twoheadrightarrow \mathscr{P}(A)$.

Let $f : A \to \mathscr{P}(A)$.

Let $X = \{a \in A \mid a \notin f(a)\} \in \mathscr{P}(A)$

Claim: $X \in \text{range}(f)$.

Let $a \in A$.

If $a \in X \Longrightarrow a \notin f(a) \Longrightarrow X \neq f(a)$.

If $a \notin X \Longrightarrow a \in f(a) \Longrightarrow x \neq f(a)$.

So $X \neq f(a) \forall a \in A$. $X \in \text{range}(f)$, so there does not exists a surjection $A \to \mathscr{P}(A)$. □

Number of Relations

For a finite set A, the cardinality of the number of relations on A is $2^{|A|^2}$.

Relations from A to B:

$\{\text{relations}\} \hookrightarrow \{\text{subsets of } A \times B\} = \mathscr{P}(A \times B)$

so the number of relations from A to B is $2^{|A| \cdot |B|}$

Properties of Relations

- Reflexive: $\forall x \in X, xRx$
- Symmetric: $xRy \iff yRx$
- Antisymmetric: xRy & $yRx \Longrightarrow x = y$
- Transitive: xRy & $yRz \Longrightarrow xRz$

Partial Ordering

- Reflexive, antisymmetric, transitive

Ex: $\subseteq, \supseteq, |...| = |...|$

Total Ordering

Same things as partial ordering, except everything must be related to each other.

$$\forall x, y \in X \text{ either } xRy \text{ or } yRx \tag{11}$$

Eg: $\leq, \geq$ on $\mathbb{R}$.

Equivalence

- Reflexive, symmetric, transitive.

$$\begin{gathered} x \equiv y (\operatorname{mod} n) \\ \Updownarrow \\ x \underset{n}{\equiv} y \Longleftrightarrow x = y + nk \text{ for some } k \end{gathered} \tag{12}$$

This is an equivalence relation.

Proof: Reflexive:

$$\begin{gathered} a \in \mathbb{Z} \\ a - a = nk \quad k = 0 \\ 0 = 0n \Longrightarrow a \underset{n}{\equiv} a \end{gathered} \tag{13}$$

Symmetric:

$$\begin{gathered} a, b \in \mathbb{Z} \\ a \underset{n}{\equiv} b \quad a - b = nk \\ b \underset{n}{\equiv} b \quad b - a = nk \end{gathered} \tag{14}$$

Transitive:

$$\begin{gathered} a, b, c \in \mathbb{Z} \\ a \underset{n}{\equiv} b \qquad\qquad b \underset{n}{\equiv} c \\ a - b = nk \qquad b - c = nl \\ a - c = n\underbrace{(k + l)}_{\in \mathbb{Z}} \\ \Longrightarrow a \underset{n}{\equiv} c \end{gathered} \tag{15}$$

□

Equivalence Classes

X a set, $\sim$ an equivalence relation on X, $x \in X$. An equivalence class of x is a subset of X.

$$[x]_{\sim} := \{y \in X \mid y \sim x\} \subseteq X \tag{16}$$

Ex:

$$\begin{gathered} [0]_{\underset{2}{\equiv}} = \{... - 4, -2, 0, 2, 4, ...\} \\ [1]_{\underset{2}{\equiv}} = \{... - 1, -1, 1, 3, ...\} \end{gathered} \tag{17}$$

$$\begin{gathered} x \sim y \Longleftrightarrow [x] = [y] \\ x \nsim y \Longleftrightarrow [x] \cap [y] = \emptyset \end{gathered} \tag{18}$$

Quotient Set

$$(X/ \sim) = \{\text{equiv of } \sim\} \tag{19}$$

Ex:

$$\begin{gathered} \left(\mathbb{Z}/ \underset{3}{\equiv}\right) = \{[a] \mid a \in \mathbb{Z}\} = \{[0], [1], [2]\} \\ \left(\mathbb{Z}/ \underset{n}{\equiv}\right) = \{[0], [1], [2], ..., [n-1]\} \end{gathered} \tag{20}$$

Modular Arithmetic

$$\left(\mathbb{Z}/ \underset{n}{\equiv}\right) = \mathbb{Z}_n \tag{21}$$

$$\begin{gathered} [a] + [b] := [a + b] \\ [a] \cdot [b] := [a \cdot b] \end{gathered} \tag{22}$$

We can do this because addition and multiplication makes sense and keeps us in the "correct" equivalence class.

Claim:

$$\begin{gathered} a \underset{n}{\equiv} a' \quad b \underset{n}{\equiv} b' \\ \Longrightarrow a + b \underset{n}{\equiv} a' + b' \\ ab \underset{n}{\equiv} a'b' \end{gathered} \tag{23}$$

Proof: (1) Suppose $a \underset{n}{\equiv} a', b \underset{n}{\equiv} b'$.

$$\begin{aligned} &\Longrightarrow aa' = nk \quad bb' = nl \quad \text{for some } k, l \in \mathbb{Z} \\ &\Longrightarrow a - a' + b - b' = n(k + l) \\ &\Longrightarrow (a + b) - (a' + b') = n(k + l) \\ &\Longrightarrow a + b \underset{n}{\equiv} a' + b' \end{aligned} \tag{24}$$

(2) Suppose $a \underset{n}{\equiv} a', b \underset{n}{\equiv} b'$.

$$\begin{aligned} a = a' + nk \quad b &= b' + nl \\ ab &= (a' + nk)(b' + nl) \\ &= a'b + n^2lk + b'nk + a'nl \\ ab - a'b' &= \underbrace{n(nkl + b'k + a'l)}_{\mathbb{Z}} \\ ab &\underset{n}{\equiv} a'b' \end{aligned} \tag{25}$$

□